(19) Japan Patent Office (JP)

## (12) Published Patent Gazette (A)

(11) Publication Number: H08-070300

(43) Date of Publication: Mar. 12, 1996

| (51) Int. Cl. | Identification Codes | JPO Ref. No | F I | | Invention Indicated |
|---|---|---|---|---|---|
| H04L 12/28 | | | | | |
| 12/40 | | | H04L 11/00 | 310 D | |
| | | | | 320 | |

Examination Not Requested, 7 Claims, OL (Total of 18 Pages)

(21) Application Number: H06-204746

(22) Application Date: Aug. 30, 1994

(71) *Applicant* -- 000003078
Toshiba Corp.
72 Horikawa-cho Saiwai-ku Kawasaki-shi Kanagawa-ken

(72) *Inventor*-- Toshio Shirakihara
Toshiba Corp. Research and Development Center
1 Komukai Toshiba-cho Saiwai-ku Kawasaki-shi Kanagawa-ken

(72) *Inventor* --Hiroshi Ezaki
Toshiba Corp. Research and Development Center
1 Komukai Toshiba-cho Saiwai-ku Kawasaki-shi Kanagawa-ken

(74) *Agent* -- Kensuke Norichika

(54) **[Name of Invention]** Network System and File Sharing Method

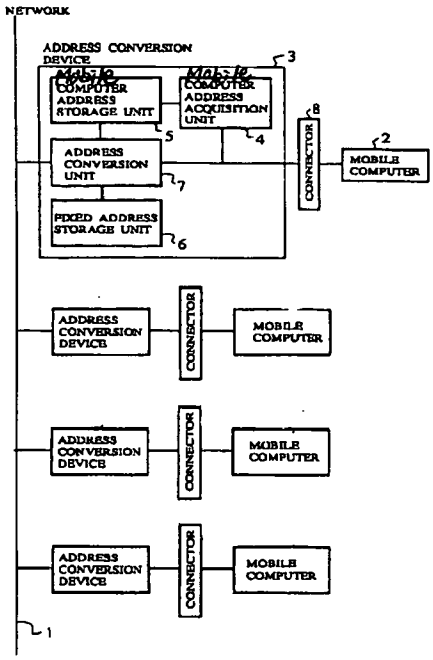
(57) **[Abstract]**

**[Objective]** An object of the present invention is to share files possessed by each mobile computer among computers on a temporarily formed network.

**[Configuration]** An address conversion device that is capable of storing a fixed address on a network, acquiring/storing an address for a mobile computer connected to the network, and address conversion using said fixed address and said mobile computer address is provided in correspondence to each connector on the network to which a mobile computer is connected. Message transmission among mobile computers is achieved by said address conversion using an assigned source address and an assigned destination address.

Eggleston Exhibit 1003
Lazaridis v. Eggleston
Interference No. 105,700

Eggleston Resubmitted Exhibit 1003
Lazaridis v. Eggleston
Interference No. 105,700




**What is claimed is:**

[Claim 1] A network system, comprising:

a network;

connector means for connecting a computer to the network;

fixed address storage means for storing a fixed address on the network corresponding to the connector means;

computer address acquisition and storage means for acquiring and storing a computer address connected to the connector means; and

means for converting an address contained in a message for a communication between the computer and the network according to the stored fixed address or the computer address.

[Claim 2] A network system having a plurality of address conversion means formed in correspondence to a plurality of connector means for connecting computers to the network, wherein said address conversion means comprising:

fixed address storage means for storing a fixed address on the network corresponding to said address conversion device;

computer address acquisition and storage means for acquiring and storing address of a computer connected to said connector corresponding to said each address conversion device; and

conversion means for converting a source address contained in a message transmitted from said computer to the network into the fixed address stored in the fixed address storage means; and

conversion means for converting a destination address contained in a message transmitted from the network to said computer into the computer address stored in the computer address acquisition and storage means.

[Claim 3] The network system of claim 2, wherein:

said computer address acquisition and storage means acquires and stores a correspondence between a computer address of another computer connected at another connector means corresponding to another address conversion device and a fixed address on the network corresponding to said another address conversion means; and

said conversion means also converts a destination address contained in the message transmitted from said computer into the fixed address according to said correspondence stored in the computer address acquisition and storage means.

[Claim 4] The network system of claim 2, wherein:

the fixed address storage means also stores a correspondence between a physical location identifier identifying a physical location of said connector means corresponding to said address conversion device and the fixed address corresponding to said each address conversion device; and

conversion of a destination address contained in the message transmitted from said computer to the network to a fixed address according to the correspondence stored in the fixed address storage means.

[Claim 5] The network system of claim 2, wherein when the address conversion means does not store the computer address connected to the connector means corresponding to the address conversion means, the conversion means sends a message with unspecified destination to said connector means and the computer address, and the computer address is acquired from a response to said message with unspecified destination issued by said computer.

[Claim 6] A file sharing method, wherein data is returned in response to an access request when other computers/users request access for files/directories stored in a computer, comprising the steps of:

assigning visible/hidden on each file/directory in advance with respect to other computers/users;

selecting only those visible files/directories to said other computers/users among files/subdirectories subordinate to said requested directory when other computers/users request access for files/directories;

reconstructing said directory data based on said selection; and
returning said reconstructed directory data in response to said access request.
[Claim 7] The file sharing method of claim 6, wherein access is controlled for files subordinate to the directories/subdirectories, comprising the steps of:
assigning access right indicating whether each file/directory possessed by each said computer is accessible from other computers/users along with assigning said files/directories to be visible/hidden in advance;
selecting the visible files/subdirectories subordinate to the said requested directory according to the visible/hidden setting;
reconstructing directory data by using selected files/directories; and
returning the reconstructed directory data.
[0001]
**[Industrial Field of the Invention]** This invention relates to a network system for network communication among mobile computers and file sharing among computers through a temporarily formed network.
[0002]
**[Description of the Background Art]** Conventionally, a file sharing scheme for sharing files among a plurality of computers has been achieved in a form of a distributed file system, etc. by forming a distributed system to which each computer is connected through a network. When a plurality of mobile computers participate in such network and share data among the mobile computers, the following procedure is necessary.

(1) Connection of each mobile computer to the network

(2) Authentication of each mobile computer/user on the network

(3) File disclosure to other users

The conventional methods and problems for respective procedures above are described in the following.

(1) Connection of each mobile computer to the network

Most of the computer networks connect fixed computers (referred hereafter as home network), in which a logical address is assigned, and comprises an address table with the correspondence between a physical address and an assigned logical address of each computer.

The procedures for a certain user U1 on a computer M1 to communicate with another computer M2 are as follows.

(a) The user U1 assigns the logical address IP2 to the computer M2.

(b) The operating system (OS) of the computer M1 searches the physical address E2 corresponding to the logical address IP2 from the address table, and then assigning the physical address E2 in order to transmit messages through the network.

[0003] In procedure (a), means for obtaining a logical address of a host from a host name is often provided, where the user assigns the host name of the computer M2 to achieve communication.

[0004] It is preferable to connect the mobile computer such as a portable computer terminal to the network other than the home network (referred hereafter as a temporary network) to which it originally belongs. As one of the methods to achieve such connection, a protocol called VIP is used based on Fumio Teraoka, Kim Claffy, and Mario Tokoro: "Design, Implementation, and Evaluation of Virtual Internet Protocol." This VIP is used to support a mobile computer on the Internet, in which the mobile computer has an IP address corresponding to the conventional logical address and a VIP address as a host identifier independent from the network to which it belongs such that the mobile transparency of the computer is achieved by using the VIP address as a logical address. By means of this protocol, the mobile computer itself can be in a similar condition as it is on the home network, but it is impossible to carry out the collaborative operation such as sharing files with other computers on the temporary network.

[005] Furthermore, another method to connect to the temporary network is to use a protocol called DHCP as disclosed in "Network Working Group: Dynamic Host Configuration Protocol, RFC (Request for Comments) 1531, October, 1993." According to DHCP, it is possible to dynamically change the network setting of the connected computer at a time of connection so that the connected computer can operate as if it is on the temporary network. However, the setting of the computer will be changed every time it is connected to a different temporary network. In addition, since the DHCP itself only provides data necessary for connecting the computer to the network, in order to actually connect the computer a software needs to be loaded so that the computer setting can be changed based on the network data obtained from the DHCP.

[006] Moreover, in the field of the Internet, an address switching IP router which switches an address of a message at a portion called router for connecting two networks has been suggested. Although it is possible to consider preparing a plurality of address switching IP routers on the

temporary network to which each mobile computer is connected, there is a drawback that it is necessary to change this static address table every time each mobile computer is connected to the temporary network because the address switch IP router switches the address in reference to a statically defined address table.

(2) Authentication of each mobile computer/user on the network

Conventionally, a distributed file system usually uses a user authentication function and a host identification function provided by a name service on the network when files are shared. For example, the identification of the user and the host in the NFS (Network File System) are carried out using the function provided by the NIS (Network Information Service). The NIS manages the data such as a host table (host name, IP address), a net group (net group name, host name), a user table (user name + pass word, user ID + group ID) etc., and the user name and the password are used to authenticate at the time of user log in. On the other hand, in the distributed file system, the disclosure of files subordinate to a certain directory is carried out by assigning host names or net group names to which the files are to be disclosed so that only the permitted hosts can access the disclosed data. Moreover, since the access right is assigned to each file, access is enabled only when user ID/ group ID is being checked and allowed to have access.

[007] There is also another method to authenticate the host and the user by managing the host table, the net group, and the user table for each computer, without using the network name service. In this case, each managed data is registered as a file in each computer.

[008] In such manner, although the conventional distributed file system enables the file sharing among computers, it aims to enable file sharing for a network configured with fixed computers such as home network. So, the computer address connected to the temporary network must be assigned by the DHCP, etc. Since such address is dynamically assigned, it is impossible to carry out authentication of each computer and there is no way to determine which data is to be disclosed.

(3) File disclosure to other users

Moreover, when disclosing files subordinate to a certain directory (referred hereafter as a disclosure root directory) to the users for the purpose of sharing the files with the other users, these files become accessible for other users as they mount the disclosure root directory. Since there are some other directories (referred hereafter as disclosure subdirectories) and some other files subordinate to the disclosure root directory, other users can know the existence of such files.

Files can only be accessed when an access right is provided. Also, when an access right is given to the disclosure subdirectory, other users can know the existence of the files and directories subordinate to such disclosure subdirectory.

[009] When setting up a certain disclosure directory on the dynamically generated network such as a temporary network, it is preferable to be able to hide the existence of particular files subordinate to the disclosure directory. However, in a conventional distributed file system, when the files subordinate to a certain directory are disclosed, the existence of all the disclosed files subordinate to that certain directory as well as the existence of the disclosed subdirectories to which the accesses are permitted are also disclosed.

[0010]

**[Problems to be Solved by the Invention]**

As aforementioned, when files in a mobile computer need to be shared among computers on a temporary network, it is possible to achieve the temporary network connection using VIP. However, the problem was the difficulty in sharing files among mobile computers. Moreover, even though mobile computers connected to the network could operate as computers on a temporary network using DHCP, it was problematic because the computer settings were changed every time mobile computers were connected to a different temporary network. Another problem was that software was required to change the computer settings based on the network data obtained from DHCP. Furthermore, it was problematic to use an address switch router because an address change table had to be changed every time mobile computers were to be connected to the network.

[0011] Furthermore, another problem was that when a distributed file system shares files, there was no means to determine which data was to be disclosed because the computer address connected to temporary network was dynamically assigned by DHCP etc.

[0012] Furthermore, when setting disclosure directory on a temporary network, while it is preferable to be able to hide the existence of particular files subordinate to the disclosure directories with respect to a user, the existence of all the files subordinate to a certain directory were disclosed when the files subordinate to a certain directory were disclosed in a conventional distributed file system. Moreover, the existence files from the disclosed subdirectories files to which the accesses were allowed were also disclosed.

[0013] It is therefore an object of the first aspect of the present invention to provide a network system capable of connecting the mobile computer to the temporary network without requiring new software on the mobile computer itself and without changing the setting of the mobile computer. Moreover, another object of the present invention is to provide a network system that is capable of communicating among mobile computers of each participant in a conference by recognizing a physical location of a mobile computer that can be used as an authentication function at a time of data disclosure.

[0014] It is therefore an object of the second aspect of the present invention to provide a file sharing method capable of disclosing different directory structures to different users/computers when files are to be disclosed to another computer. File sharing should be achieved even when different users/computers request data disclosure from the same directory.

[0015]

[Means for Resolving Problem] A network system according to the first aspect of the present invention, comprising: a network; connector means for connecting a computer to the network; fixed address storage means for storing a fixed address on the network corresponding to the connector means; computer address acquisition and storage means for acquiring and storing a computer address connected to the connector means; and means for converting an address contained in a message for a communication between the computer and the network according to the stored fixed address or the computer address.

[0016] The present invention relates to a communication method among computers through a plurality of address conversion devices formed in correspondence to a plurality of connectors for connecting computers to the network, wherein a fixed address on the network of the address conversion device is stored in advance, a computer address connected to the connectors in correspondence to the address conversion device is acquired and stored, a source address contained in a message transmitted from the computer to the network is converted into the fixed address stored in the fixed address storage means, and a destination address contained in a message transmitted from network to the computer is converted into the computer address stored in the computer address acquisition and storage means.

[0017] Furthermore, said network system comprising: means to store a correspondence between a physical location identifier for identifying a physical location of said connector means corresponding to each address conversion device and the fixed address on the network

corresponding to said each address conversion device; and a destination address contained in message transmitted from the computer to the network is converted into the fixed address with reference to said stored correspondence.

[0018] A file sharing method according to the second aspect of the present invention, wherein directory data is returned in response to the access request when another computer/user requests access for files/directories stored in a computer, comprising the steps of: assigning visible/hidden on each file/directory for other computers/users in advance; selecting only those visible files/directories to said other computers/users among files/subdirectories subordinate to said requested directory when other computers/users request access for files/directories; reconstructing said directory data based on said selection; and returning said reconstructed directory data in response to said access request.

[0019]

[Effect] According to the first aspect of the present invention, a fixed address is stored on the network, a mobile computer address in message transmitted from a mobile computer to the network by an address conversion device which acquires and stores an address of a mobile computer connected to the network, and a fixed address contained in message transmitted from the network to a mobile computer is converted into a mobile computer address. Therefore, a mobile computer regards its own computer as a source address and transmits messages by using a fixed address of an address conversion device to which other people's computers are connected as a destination address. This enables communication without having to load new software on the mobile computer itself or changing the setting itself. Other people's computer addresses can also be used as a destination address (as indicated in claim 3).

[0020] Furthermore, by having an address table corresponding to a physical location identifier and a fixed address of another address conversion device, a mobile computer can transmit a message by assigning said identifier. Therefore, a mobile computer of each user can be recognized by a physical location which enables communication and achieves the authentication function at the time of data disclosure.

[0021] According to the second aspect of the present invention, files/directories are set to be visible/hidden to another computer/a group of computer, or another user/a group of users in advance. When a certain directory data is disclosed to another computer/a group of computers, or another user/a group of users, the files/subdirectories subordinate to the directory are checked

whether they are visible/hidden with respect to each disclosure target to which the reconstructed directory data is to be disclosed. So, even when the disclosure request is made to the same directory, different structure can be disclosed to each user/computer.

[0022]

[Embodiments]

(Embodiment 1)

(Primary Components of the Scheme and Effect) A network system according to the present invention comprises an address conversion device including fixed address storage means for storing a fixed address on the network, computer address acquisition and storage means for acquiring and storing a computer address, and address conversion means using said fixed address storage means and computer address storage means. An address conversion device is provided corresponding to each connector to which computers are connected.

[0023] The address conversion device acquires the computer address of the mobile computers connected to the network, stores the acquired computer address in the computer address storing means, and stores the fixed address of that address conversion device. When computer A and computer B communicate, computer A assigns the address conversion device B to which computer B is connected to carry out communication. Address conversion device A converts the address of computer A contained in message into the fixed address stored in the fixed address acquisition means so that the message is sent to address conversion device B. Address conversion device B converts the address in address conversion means B contained in message into the address of computer B and then sending it to computer B.

[0024] (Effect) Conventionally, in a case of connecting a computer to a temporary network, there has been a need to obtain a network data such as address etc. dynamically from the network and change the setting of the computer according to the obtained network data. Also, it has been necessary to provide software to automatically change such setting. In addition, since an address conversion table is statically defined in a conventionally known address conversion method, it is not suitable for a mobile computer connected to the network dynamically.

[0025] However, according to this embodiment of the present invention, a mobile computer is connected to an address conversion device which stores a fixed address in advance, acquires and stores a computer address of the connected computer, and converts the computer address into the fixed address automatically. So, there is neither a need to provide software for changing the

setting nor a need to change the setting itself. Moreover, since each computer thinks that the network is only composed of the fixed address stored in each address conversion device, each computer only needs to recognize such fixed address. Furthermore, the computer address of each computer can be hidden from other computers connected to the same network. As the computer address of the mobile computer is dynamically acquired by the address conversion device, it becomes unnecessary to rewrite an address conversion table.

[0026] (Detailed Description) A first embodiment of the present invention is described in detail with reference to the drawings. FIG. 1 illustrates a network system scheme of this embodiment. A plurality of address conversion devices 3 that carry out address conversion of the mobile computer 2 connected to the network 1 comprise the fixed address corresponding to the network. The address conversion devices 3 are composed of the mobile computer address acquisition unit 4 acquiring address of the mobile computers 2 connected via the connectors 8 which enables wired/wireless connection, the mobile computer address storage unit 5 storing such address, and the fixed address storage unit 6 storing the fixed address of the address conversion devices 3, and the address conversion unit 7 transmitting messages among mobile computers and network by address conversion according to the fixed address and the mobile computer address. Message transmitted on the network 1 comprises a source address and a destination address. The message content will be indicated as M (source address, destination address).

[0027] As shown in FIG. 2, procedures are explained when the mobile computer 21 having the computer address a1 connected to the address conversion device 31 which stores the fixed address A1 communicates with another mobile computer 22 having the computer address a2 connected to another address conversion device 32 which stores the fixed address A2. Also, FIG. 3 is a flow chart showing procedures of an address conversion device. The mobile computer 21 and 22 assign addresses for the address conversion devices to which it is connected at the time of connection and transmit messages such as M (A1, a1) and M (A2, a2). The address conversion devices 31 and 32 acquire the mobile computer addresses from the message, and register them at the mobile address storage unit (S4). Then, the mobile computer 21 communicates with the mobile computer 22 by issuing a message M (A2, a1) to assign the address A2 of the address conversion device 32 to which the mobile computer 22 is connected. The address conversion unit of the address conversion device 31 converts a source address of message M (A2, a1) into

message M (A2, A1) using the stored fixed address A1 (S2, S3), and then the message is transmitted to the address conversion device 32 via the network. The address conversion device 32 converts a destination address of the received message M (A2, A1) to M (a2, A1) using the address a2 stored in the mobile address storage unit (S5, S6), and then the message is transmitted to the mobile computer 22. So, the mobile computer 22 receives the message from the address conversion device 31. Thus, when responding to the mobile computer 21, the message is sent to the address conversion device 21. By taking similar procedures as above operation, the message is transmitted to the mobile computer 21.

[0028] (Variant Embodiment 1) In this embodiment, the mobile computer address storage unit 5 in the scheme of FIG. 1 is arranged to have a pair of the computer address of each mobile computer and the address of a corresponding address conversion device, for all the mobile computers connected to the network. For this reason, the mobile computer address acquisition unit 51 of each address conversion device notifies a pair of the acquired computer address and the fixed address of this address conversion device to all the other address conversion device at the time of mobile computer address acquisition (FIG. 3 S4). Therefore, the mobile computer can communicate by assigning the mobile computer address rather than the fixed address from the address conversion device of the mobile computer.

[0029] The operation is described according to FIG. 4. FIG. 4, similarly to the scheme of FIG. 2, illustrates procedures when the mobile computer 21 assigns the address of the mobile computer 22 rather than the address of the conversion device 32 to be used for transmitting message. Moreover, FIG. 5 is a flow chart illustrating procedures of an address conversion device. Similarly to the procedures in FIG, 2, each mobile computer transmits messages to the address conversion device connected to the network at the time of connection. Each address conversion device notifies a pair of the computer address acquired from the message and the fixed address to all the other address conversion devices (S15). In FIG. 4, the address conversion devices 31 and 32 notify a pair of the computer address (A1, a1) and (A2, a2) to each other. In case the mobile computer 21 transmits message M (a2, a1) to the mobile computer 22, the address conversion device 31 inquires the mobile computer address storage unit 51 about the fixed address of address conversion device corresponding to a2, a1, obtains address A2, A1 corresponding to a2, a1 (S12), then converts address (S13) in order to transmit message M (A2, A1) to the address conversion device 32. The address conversion device 32 with received message inquiries the

mobile computer address storage unit about the mobile computer address corresponding to each A1, A2, obtains address a2, a1, convert address (S16, S17), and transmits address message M (a2, a1) to the mobile computer 22. Thus, the mobile computer 22 receives the message from the mobile computer 21 and transmits the response to the mobile computer 21. By taking similar procedures as above operation, the message is transmitted.

[0030] (Variant Embodiment 2) A fixed address storage unit 6 in the scheme of FIG. 1 comprises a corresponding table of physical location identifiers indicating locations of physical settings and fixed addresses of all the address conversion devices connected to the network. Mobile computers communicate by assigning said identifier so that the address conversion unit obtains the fixed address from the fixed address storage unit corresponding to the assigned identifier before address conversion takes place. Thus, it enables communication by recognizing physical locations of each participant's mobile computer at a conference etc. and can be used as authentication function at the time of data disclosure.

[0031] In other words, each participant (user) is physically facing other participants. Since each participant corresponds to each mobile computer (connected to the address conversion device set at the conference room in advance), for a user to determine to whom the data is to be disclosed is the same as to determine at which setting location of the mobile computer the data is to be transmitted. Therefore, actual face-to-face authentication reflects through the physical locations of computers whether the data is to be disclosed. From a point of view of communication among computers, data disclosure means to send data possessed by a certain user to other users in forms of messages. From a point of view of distributed file system which is achieved by communication function among computers, data disclosure means to share files by sending messages containing file data possessed by a certain user to computers of other users.

[0032] As shown in FIG 6 (a), when an address conversion device is set at a conference room etc. in advance, the fixed address storage unit 61 of each address conversion device comprises a correspondence table of identifiers indicating setting locations and fixed addresses along with what is in the fixed address storage unit 6 of FIG. 1, as shown in FIG. 6 (b). The operation is described according to a flow chart of an address conversion device shown in FIG. 6 (c) and FIG. 7. For example, suppose a user of the mobile computer 21, connecting his/her own computer to the address conversion device of setting location 1 of FIG. 6 (a), wishes to send data from his/her own computer to another user next to him/her (the computer being connected to an address

conversion device of setting location 2). In FIG. 6 (c), when the mobile computer 21 sends message to the mobile computer 22, the identifier 2 indicating setting location of the mobile computer 22 is assigned to transmit message M (2, a1), the address conversion device 31 converts the identifier 2 indicating setting location into a fixed address A2 of the address conversion device 32 (S22) with reference to a correspondent table of the FIG. 6 (b), a source address a1 is converted into A1 with reference to what is in the fixed address storage unit 6 (S23), and then message M (A2, A1) is transmitted to the address conversion device 32. The address conversion device 32 then converts a source address A1 of the message into the identifier 1 indicating setting location (S26), and converts a destination address into address a2 of the mobile computer 22 (S27) so that it is transmitted to the mobile computer 22. Said process enables each mobile computer to communicate with other mobile computers by only recognizing the identifiers such as seating numbers etc.

[0033] (Variant Embodiment 3) In this embodiment, means to transmit address unspecified message to a mobile computer is added to the address conversion unit 7 of the scheme of FIG. 1 such that the mobile computer address can be acquired from the first message issued by the mobile computer of the mobile computer address acquisition unit 4. Address that is supposed to be stored in the mobile computer address storage unit 5 can be acquired either from the first message from the mobile computer or when mobile computer address is not stored at the mobile computer address storage unit at the time of converting address of message from other address conversion device, an unspecified message is sent to the mobile computer so that the mobile computer address can be obtained from its response. Thus, mobile computer address acquisition is enabled without transmitting message to the address conversion device which is used at the time of connecting mobile computer.

[0034] Since message is transmitted to a computer with unspecified address in many networks, means to request response is provided. For Internet, when broadcasting is conducted (transmission of address unspecified message) according to a protocol called ICMP, responses can be obtained from all the computers connected to the Internet. In this embodiment, said means is applied when address conversion device does not know the mobile computer address connected to one's own connector, address conversion unit transmits address unspecified message toward connector 8 so that response is returned from mobile computer currently being connected to address conversion device.

[0035] Procedures are described with reference to the flow chart of FIG. 8 and FIG. 9. The mobile computer 21 transmits M (A2, a1) to the address conversion device 31 in order to communicate with mobile computer 22. In case address conversion device 31 does not store address for mobile computer 21 (S31 NO), address for mobile computer 21 is obtained and stored at mobile computer address storage unit 5 (S32), address conversion is conducted similar to FIG. 1 (S22, S34) and transmits M (A2, A1) to address conversion device 32. Although address conversion device 32 wishes to convert destination address to address a2 of mobile computer 22, if the address a2 is unknown (not stored), address unspecified message M (al, A1) is sent to the mobile computer 22 and the address of mobile computer 22 is obtained from received M (A2, a2) (S36), and then address conversion is conducted similar to FIG. 1.

(Embodiment 2)

(Primary Elements of the Configuration and its Effect)

A distributed file system in this embodiment (a system configured with a plurality of computers where a computer registers each file in a directory structure and a certain computer can have access to files in another computer) comprises; means to assign files/directories as visible/hidden with respect to another computer/a group of computers, another user/a group of users; and means to reconstruct directory data after determining whether files/subdirectories subordinate to the directory is visible/hidden to a disclosed user.

[0036] Owner of file/directory specifies whether each file/directory can be disclosed to another computer/a group of computers, another user/a group of users, and access right is checked upon access request for the directory so that only visible files/directories subordinate to the directory is used to reconstruct disclosure data and disclosed to others. Meaning of this data disclosure is mentioned in a second variant embodiment of a first embodiment.

[0037] (Effect) In the conventional distributed file system, when a certain directory is disclosed, the existence of files/directories subordinate to the directory was known to other users as well. However, by providing means for visible/hidden setting for files/directories subordinate to the structure of disclosed directory structure, directory data is reconstructed depending on whether it is visible/hidden so that different structure can be disclosed for the same directory requested by each user/computer.

[0038] (Relationship of Embodiment 1 and Embodiment 2) From implementation point of view, data disclosure in a distributed file system of a second embodiment is achieved by

communication using computer addresses from source disclosure and destination disclosure. However, when mobile computer is included in the computer system loaded with a distributed file system, at implemented level communication can be achieved by the embodiment 1 format. Particularly, when an address conversion device, a connector of a second variant embodiment of embodiment 1, and a computer incorporated by the file system of embodiment 2 are combined as a mobile computer, authentication of the destination disclosure can be carried out because each user is face-to-face to each other. This also enables to assign visible/hidden for files per each user. For instance, if someone assigns visible/hidden to each setting location per each file (described as computer ID of a second embodiment), only file F1 is disclosed to the user at location setting 3 and only file F1 and file F2 are disclosed to the user at location setting 2 (physically, it is a message transmission among computers using the address conversion among setting location, the fixed address of the address conversion device, and the computer address).

[0039] (Detailed Description) Second embodiment of the present invention is described with reference to the figures. FIG. 10 shows a network system scheme in this embodiment. Each computer 11 comprises the data disclosure unit 12 that discloses data (files/directories) stored in each computer, the data mount unit 13 that requests other computers to provide and import data, and the file system 14 that manages data. The file system, as shown in FIG. 11, has a plurality of files/subdirectories and visible/hidden files which used to set the files/subdirectories as visible/hidden. Further, the similar structure exists for the files subordinate to the subdirectory. Visible/hidden files, as shown in FIG. 12, define visible users/hosts for each file subordinate to directory.

[0040] In FIG. 10, the computer 1 has a structure subordinate to the directory D1 shown in FIG. 11. Procedures are explained in a flow chart of FIG. 13 when the computer 2 requests data subordinate to directory D1. The data mount unit 13 of the computer 2 assigns host 2 as the computer ID in order to request data (S41). The data disclosure unit 12 of the computer 1 reconstructs the directory data indicating the existence of file F1 and file F2 subordinate to directory D1 according to the visible/hidden file data in the directory 1 (S42, S43), and returns reconstructed directory data to the data mount unit 13 of the computer 2 (S44). The computer 2 with returned directory data then accesses the file F1 or the file F2 according to the conventional access right setting mentioned later so that the files in computer 1 can be shared.

[0041] In the above, it is assumed that the usual access right for the directory D1 is in a readable setting for the computer 2. That is, this embodiment first checks the access right for the requested directory, and when it is in a readable setting, the visible/hidden file for the requested directory is checked so that only those visible files/ directories subordinate to the requested directory are returned. When the requesting computer further requests a specific data from the returned data, the similar procedure is repeated.

[0042] (Variant Embodiment) Instead of using method to assign visible/hidden to files in FIG. 8, expanded access settings for each file/directory are used.

[0043] Access rights such as readable, writable, and executable settings can be assigned to three types of targets including an owner, a group, and others the access control for files provided by the conventional UNIX. These access rights are expanded to include four settings such as readable, writable, executable, and visible settings, and at a time of the disclosure of directory data, the data disclosure unit carries out the reconstruction of the directory data by selecting the visible files according to the access rights for all the files and directories subordinate to the requested directory instead of the procedures of S42.

[0044] Access control that is more flexible than the conventional UNIX is achieved by using the ACL (Access Control List). In the ACL, the access right for each file can be set as follows.

user: foo1: rwxci

group: foo2: r----

In the above setting, with respect to the user called "foo1", the access right indicates five settings including readable (r), writable (w), executable (x), ACL changeable (c), and insertable (i) while, the access right indicates only readable (r) as a setting for the group called "foo2". In addition to these attributes of the access right, a new attribute of visible (v) is added so that directory data reconstructs similarly to the above procedure.

[0045] In this manner, even when the directory data has changed due to the shift or the deletion of the files, it is possible to disclose different structures to different users/ computers without requiring an editing etc. of the visible/hidden files.

[0046] [Effect of the Invention] A first aspect of the present invention enables a network communication scheme capable of connecting the mobile computer to the temporary network without requiring new software on the mobile computer or changing the setting of the mobile computer. Moreover, a network system with a network communication scheme can be utilized

as an authentication function at a time of disclosing the data by recognizing physical locations of mobile computers of each participant in a conference etc.

[0047] Further, according to a second aspect of the present invention when files are disclosed to other computers, even if they are in the same directories, it is possible to disclose different directory structures for each user /computer.

**[Brief Description of the Drawings]**

FIG. 1 is a diagram illustrating a network communication scheme of a first embodiment according the present invention.

FIG. 2 is a block diagram showing a summary of the communication procedures among mobile computers.

FIG. 3 is a flow chart illustrating procedures for an address conversion device of FIG. 2.

FIG. 4 is a block diagram illustrating communication procedures of a first variant embodiment 1 according to a first embodiment of the present invention.

FIG. 5 is a flow chart illustrating procedures for an address conversion device of FIG. 4.

FIG. 6 is a block diagram illustrating communication procedures of a second variant embodiment 1 according to a first embodiment of the present invention..

FIG. 7 is a flow chart illustrating procedures for an address conversion device of FIG. 6.

FIG. 8 is a block diagram illustrating communication procedures of a third variant embodiment according to a first embodiment of the present invention

FIG. 9 is a flow chart illustrating procedures for an address conversion device of FIG. 8.

FIG. 10 is a diagram of a network communication scheme of a second embodiment according to the present invention.

FIG. 11 illustrates a file system scheme of the computer 1 of FIG. 10.

FIG. 12 is a chart shows what is in visible/hidden files of FIG. 11.

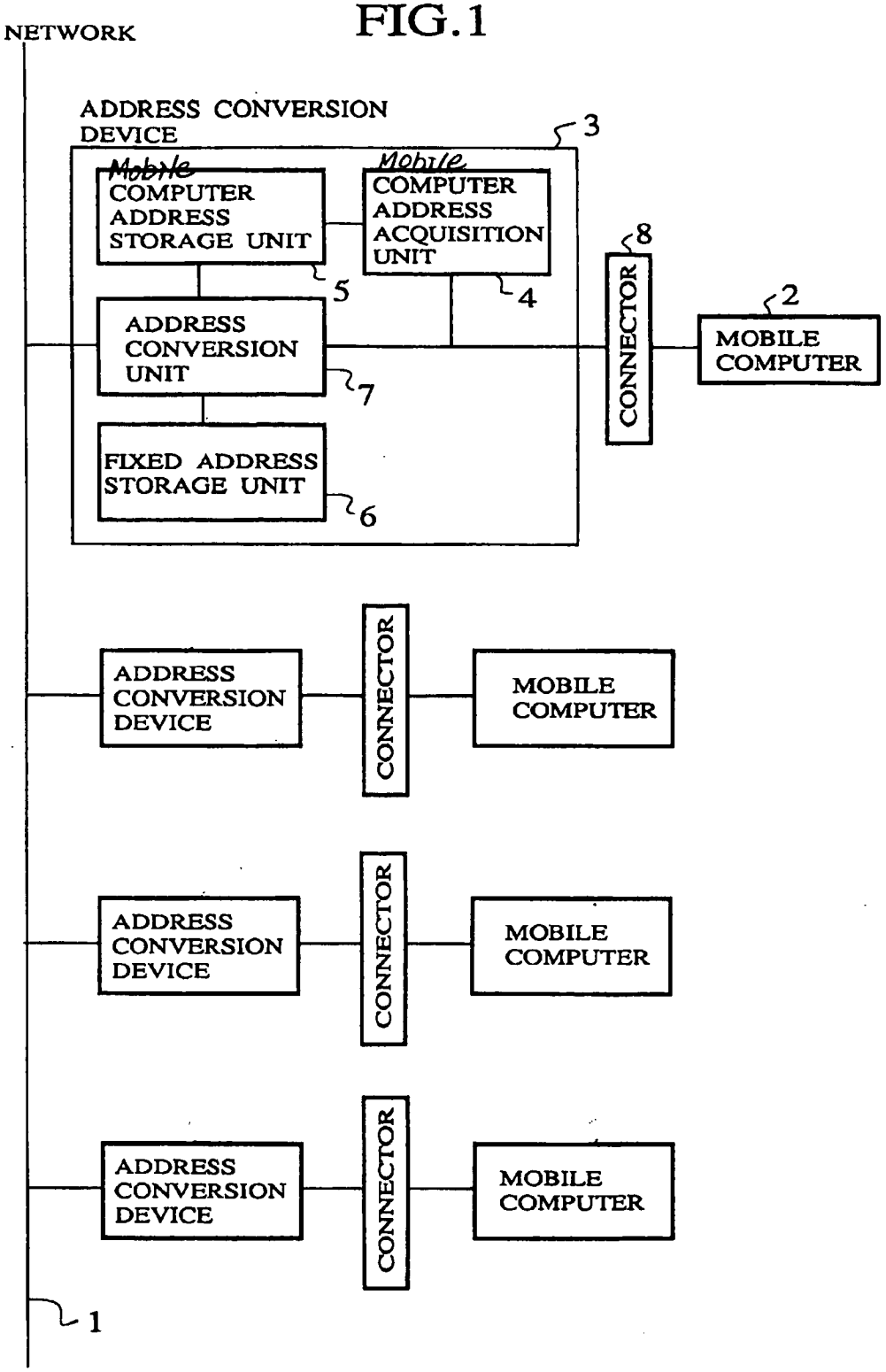
FIG. 13 is a flow chart showing procedures of data disclosure unit and data mount unit of FIG. 10.

**[Description of Notations]**

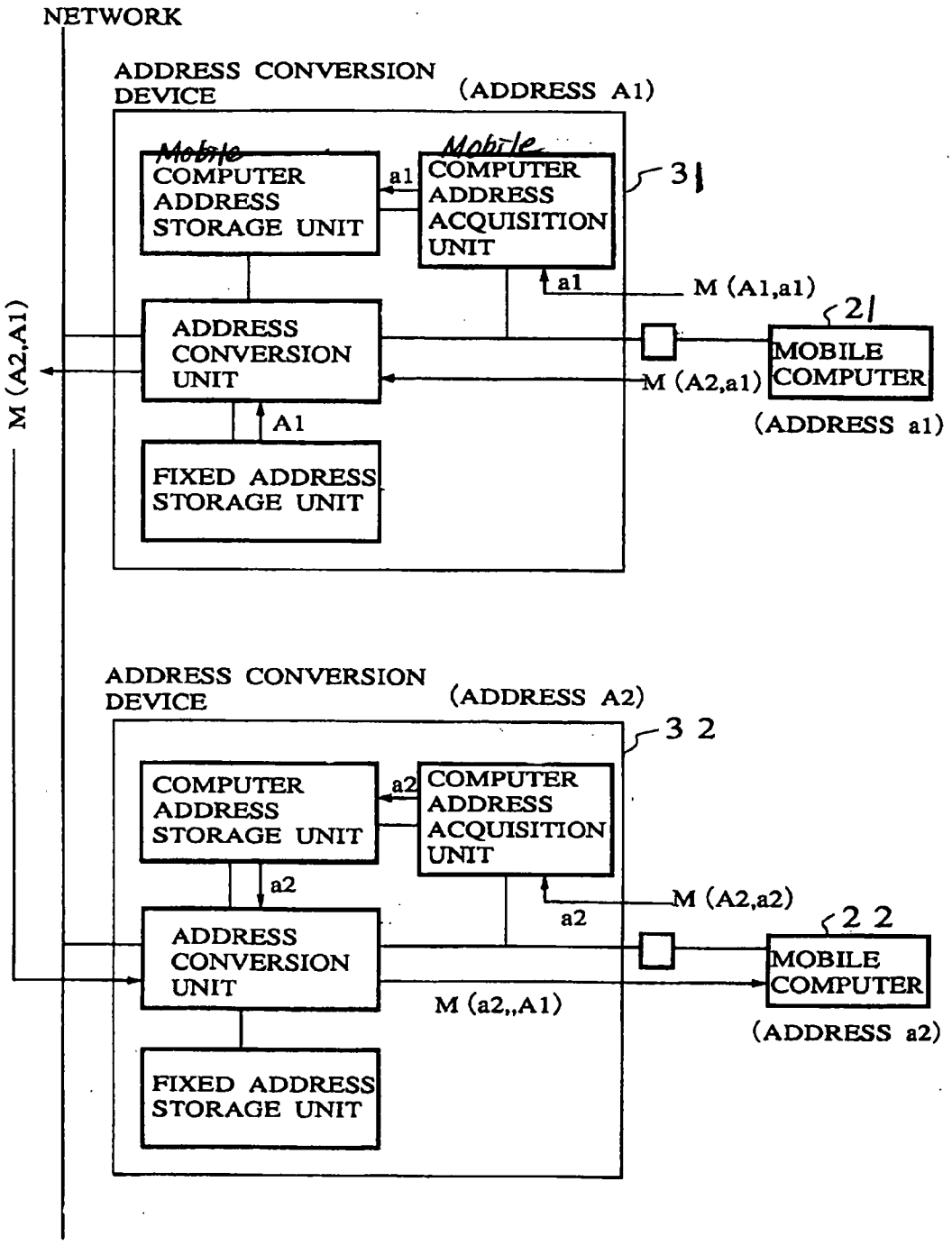
1 Network
2, 21, 22 Mobile computer
3, 31, 32 Address Conversion Device
4, 41 Mobile Computer Address Acquisition Unit
5, 51 Mobile Computer Address Storage Unit
6, 61 Fixed Address Storage Unit

7, 71 Address Conversion Unit
8 Connector
11 Computer
12 Data Disclosure Unit
13 Data Mount Unit
14 File System

FIG.1

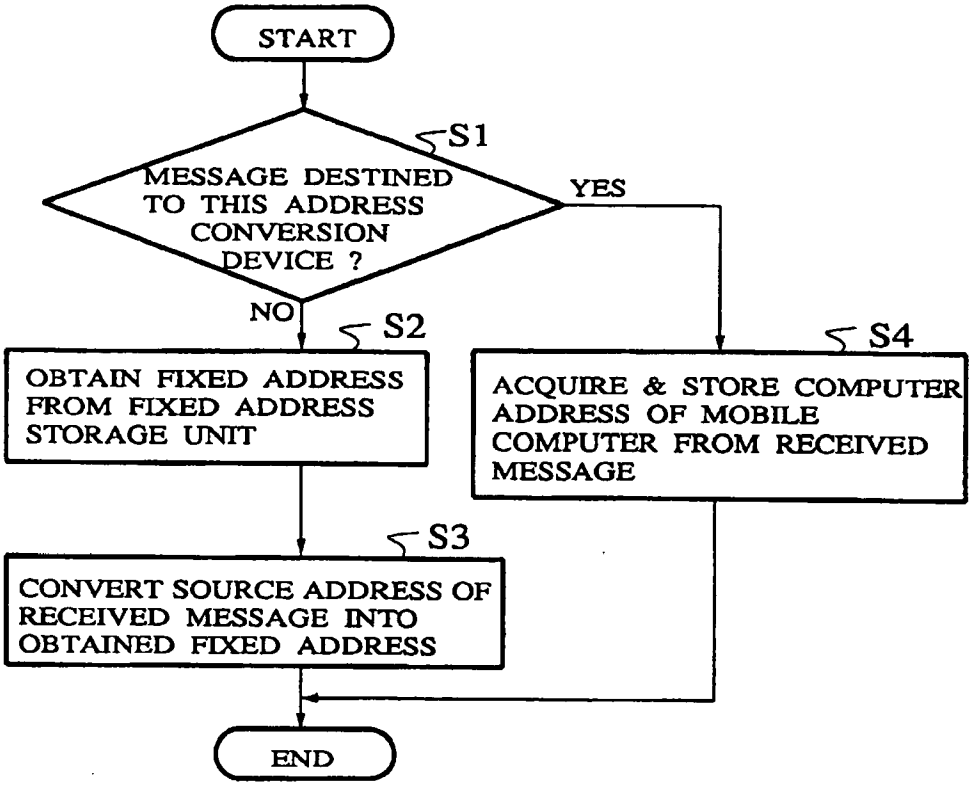

NETWORK
ADDRESS CONVERSION DEVICE
3
Mobile COMPUTER ADDRESS STORAGE UNIT
5
Mobile COMPUTER ADDRESS ACQUISITION UNIT
4
ADDRESS CONVERSION UNIT
7
FIXED ADDRESS STORAGE UNIT
6
8
CONNECTOR
2
MOBILE COMPUTER
ADDRESS CONVERSION DEVICE
CONNECTOR
MOBILE COMPUTER
ADDRESS CONVERSION DEVICE
CONNECTOR
MOBILE COMPUTER
ADDRESS CONVERSION DEVICE
CONNECTOR
MOBILE COMPUTER
1

# FIG.2

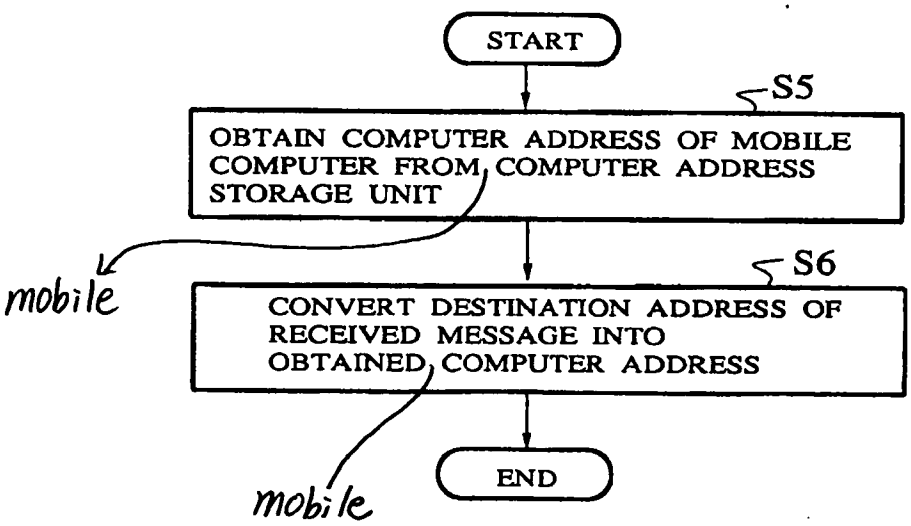

NETWORK
ADDRESS CONVERSION DEVICE
(ADDRESS A1)
COMPUTER ADDRESS STORAGE UNIT
a1
COMPUTER ADDRESS ACQUISITION UNIT
31
a1
M (A1,a1)
21
ADDRESS CONVERSION UNIT
M (A2,A1)
M (A2,a1)
MOBILE COMPUTER
(ADDRESS a1)
A1
FIXED ADDRESS STORAGE UNIT
ADDRESS CONVERSION DEVICE
(ADDRESS A2)
32
COMPUTER ADDRESS STORAGE UNIT
a2
COMPUTER ADDRESS ACQUISITION UNIT
a2
M (A2,a2)
22
ADDRESS CONVERSION UNIT
M (a2,,A1)
MOBILE COMPUTER
(ADDRESS a2)
FIXED ADDRESS STORAGE UNIT

# FIG. 3

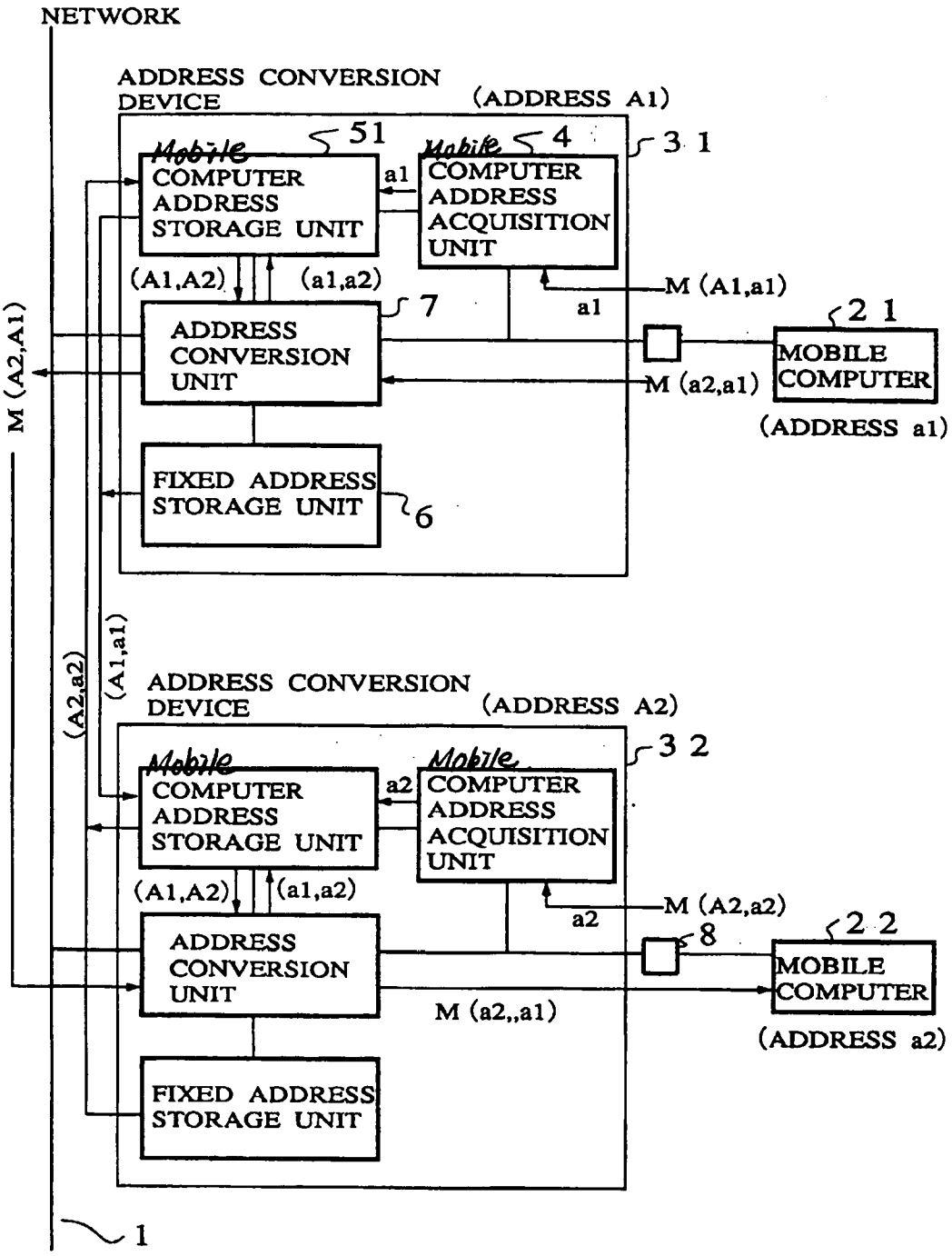
[Message from Mobile Computers]




[Message from Other Address Conversion Devices]

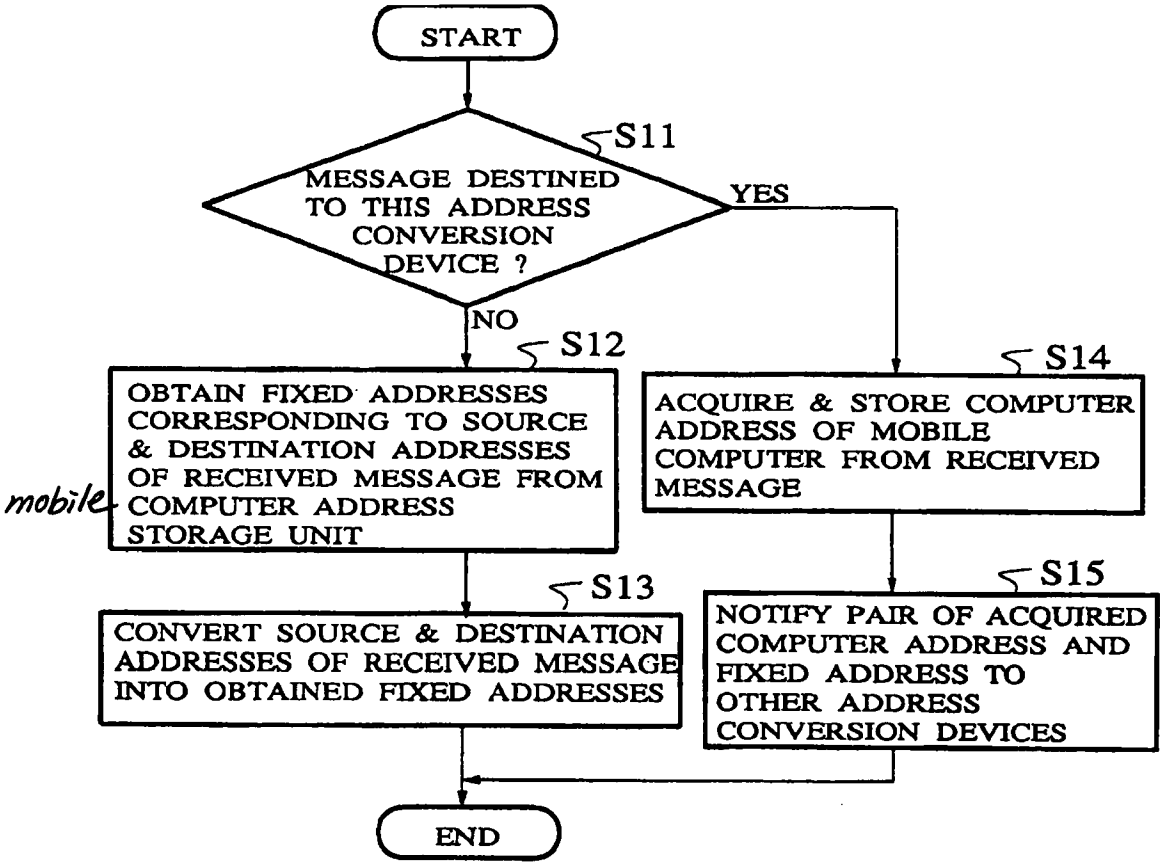


# FIG. 4

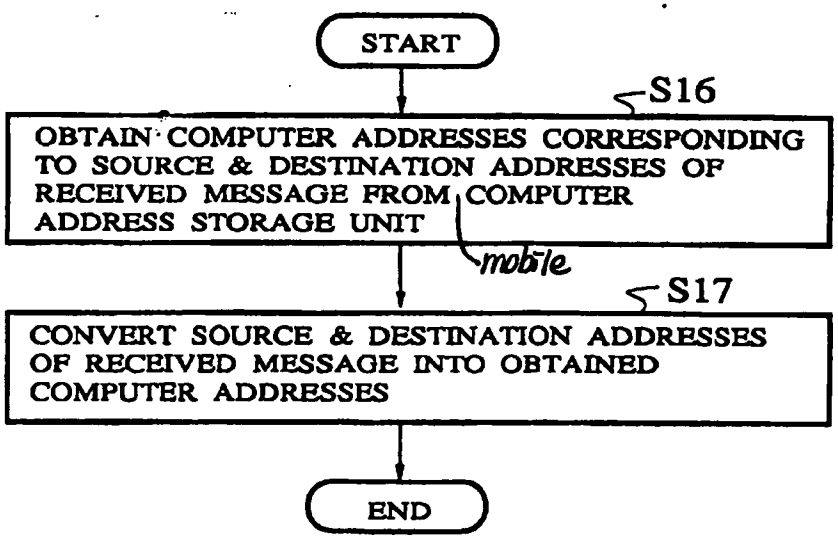

NETWORK
ADDRESS CONVERSION DEVICE
(ADDRESS A1)
51
4
3 1
Mobile COMPUTER ADDRESS STORAGE UNIT
a1
Mobile COMPUTER ADDRESS ACQUISITION UNIT
(A1,A2)
(a1,a2)
7
M (A1,a1)
a1
2 1
ADDRESS CONVERSION UNIT
M (a2,a1)
MOBILE COMPUTER
(ADDRESS a1)
M (A2,A1)
FIXED ADDRESS STORAGE UNIT
6
(A1,a1)
(A2,a2)
ADDRESS CONVERSION DEVICE
(ADDRESS A2)
3 2
Mobile COMPUTER ADDRESS STORAGE UNIT
a2
Mobile COMPUTER ADDRESS ACQUISITION UNIT
(A1,A2)
(a1,a2)
M (A2,a2)
a2
8
2 2
ADDRESS CONVERSION UNIT
M (a2,,a1)
MOBILE COMPUTER
(ADDRESS a2)
FIXED ADDRESS STORAGE UNIT
1

# FIG. 5

[Message from Mobile Computer]

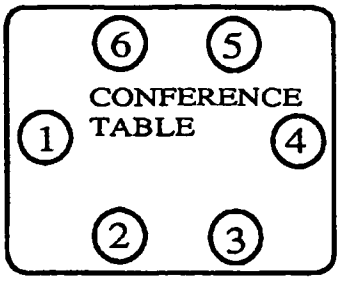



[Message from Other Mobile Computers]



# FIG. 6

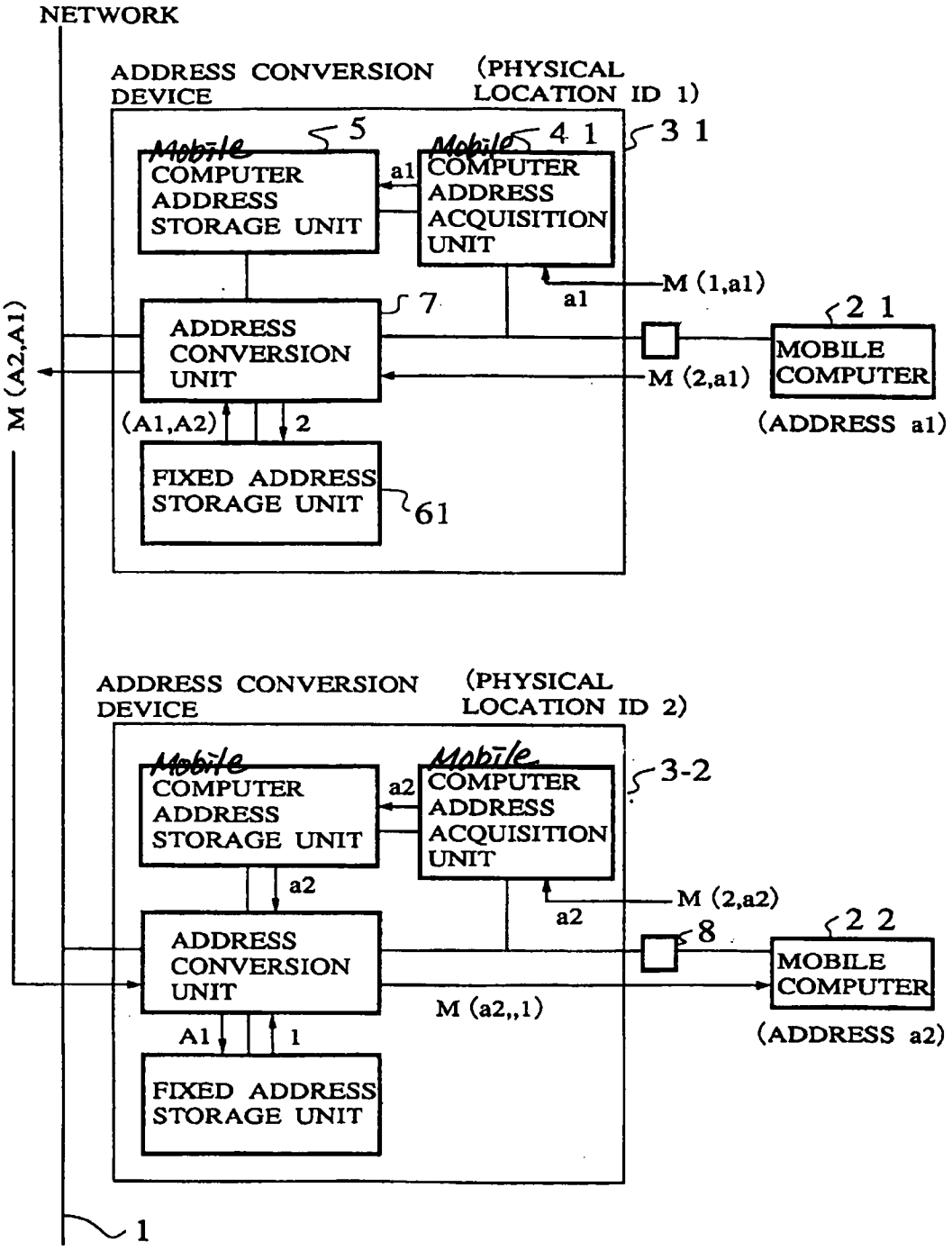
(a) Setting Locations of Address Conversion Devices




(b) Correspondent Table of Setting Location Identifier and Fixed Address

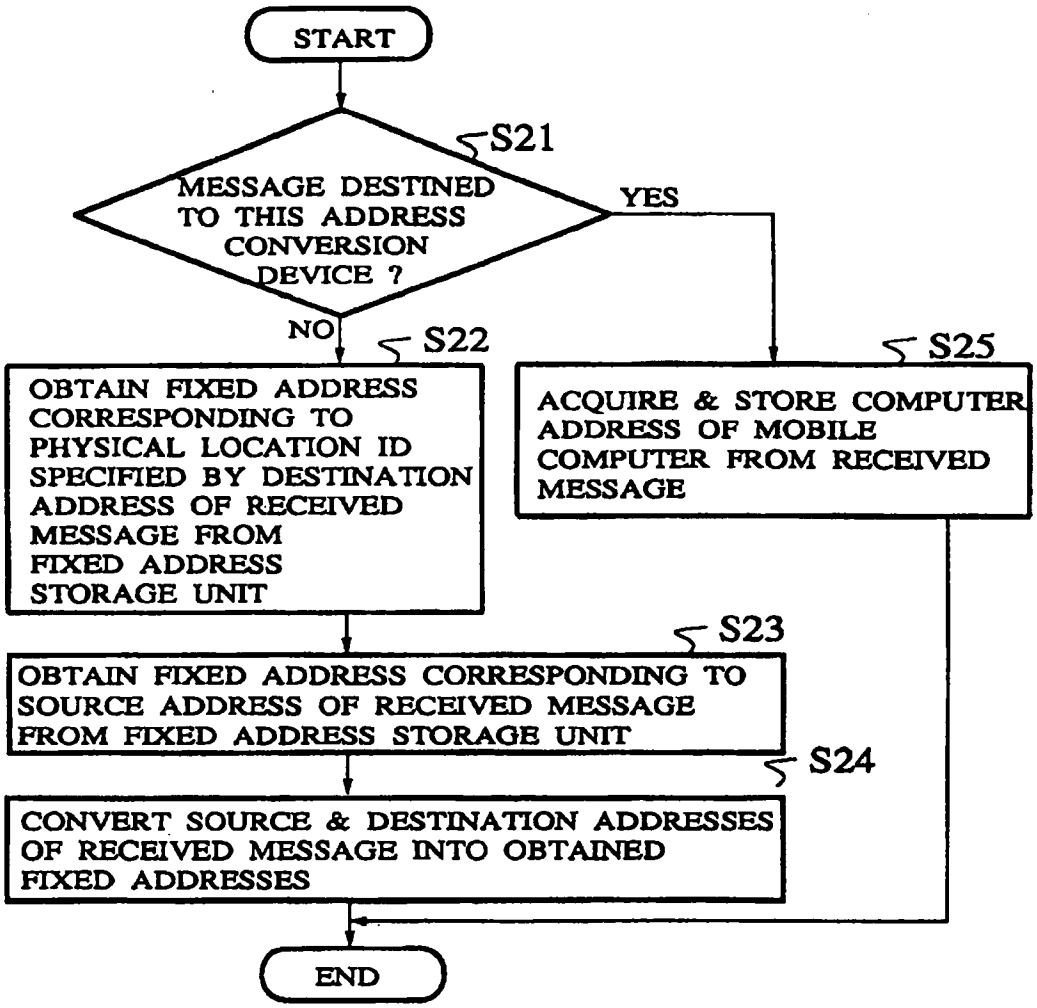
| PHYSICAL LOCATION ID | FIXED ADDRESS |
|---|---|
| 1 | A1 |
| 2 | A2 |
| 3 | A3 |
| | |
| | |

(c) Procedures

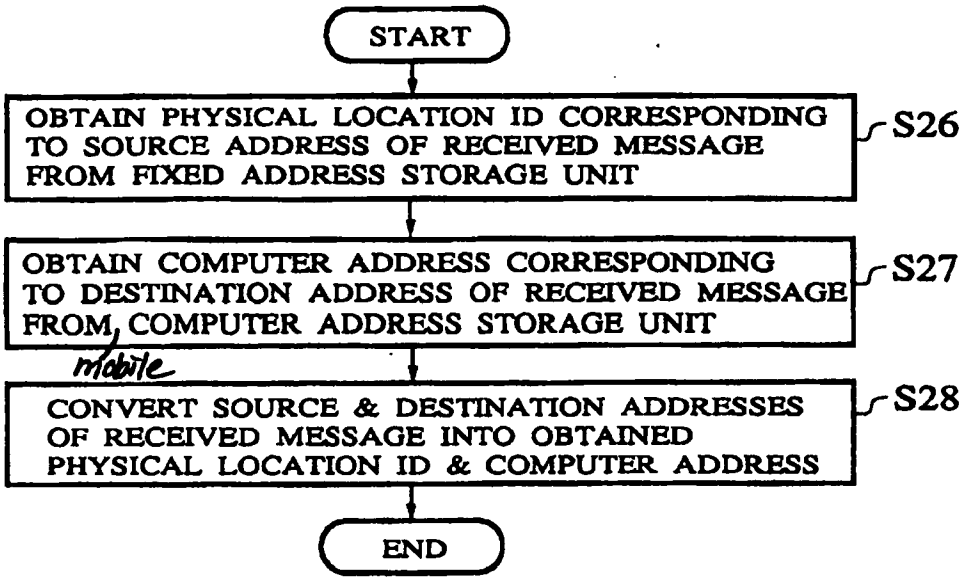


# FIG. 7

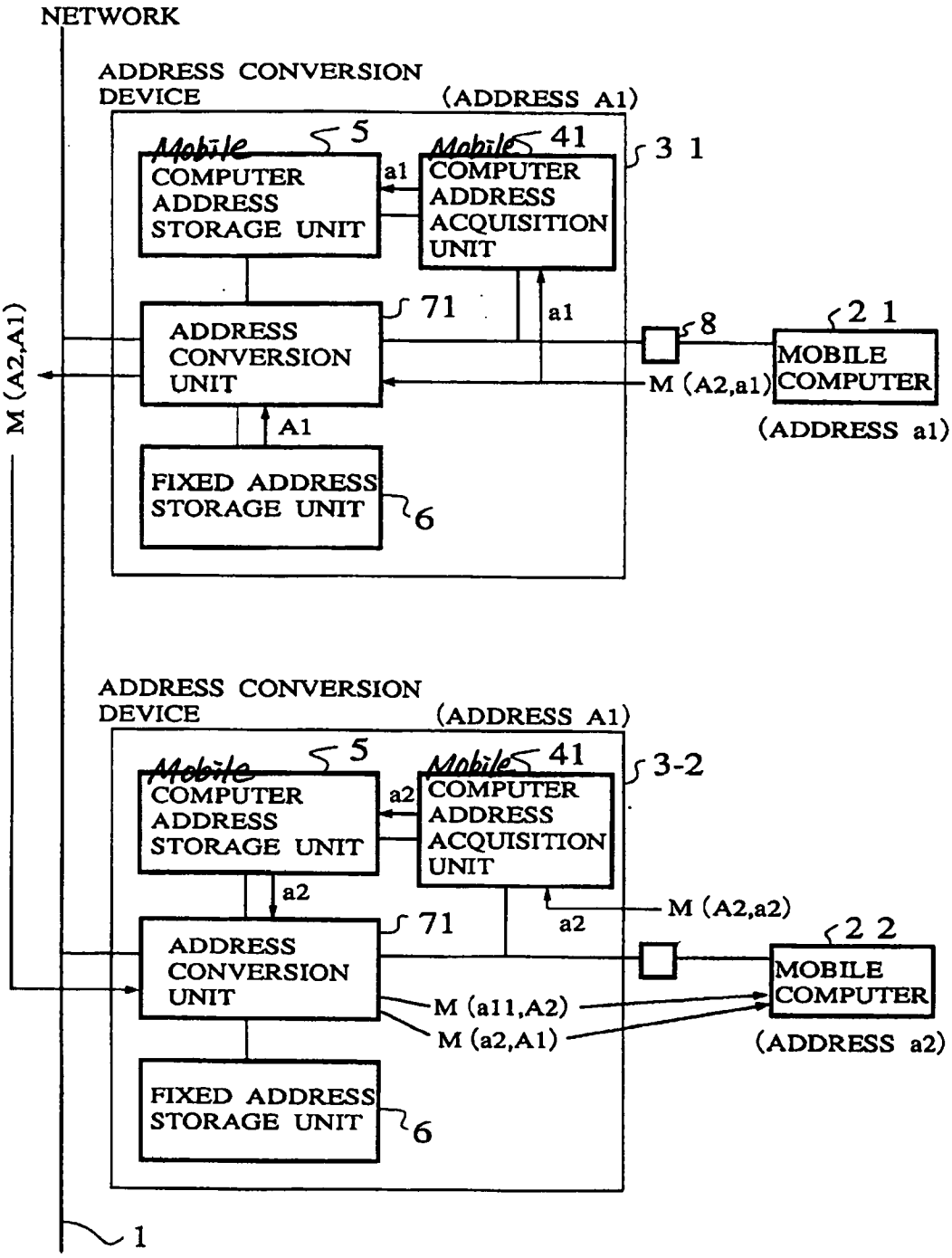
[Message from Mobile Computer]



[Message from Other Address Conversion Devices]

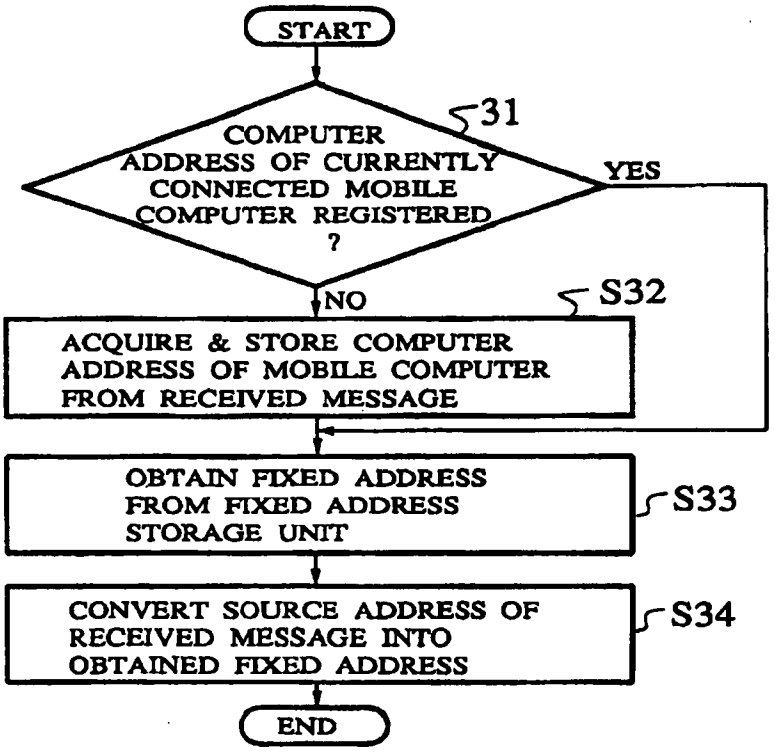


# FIG. 8

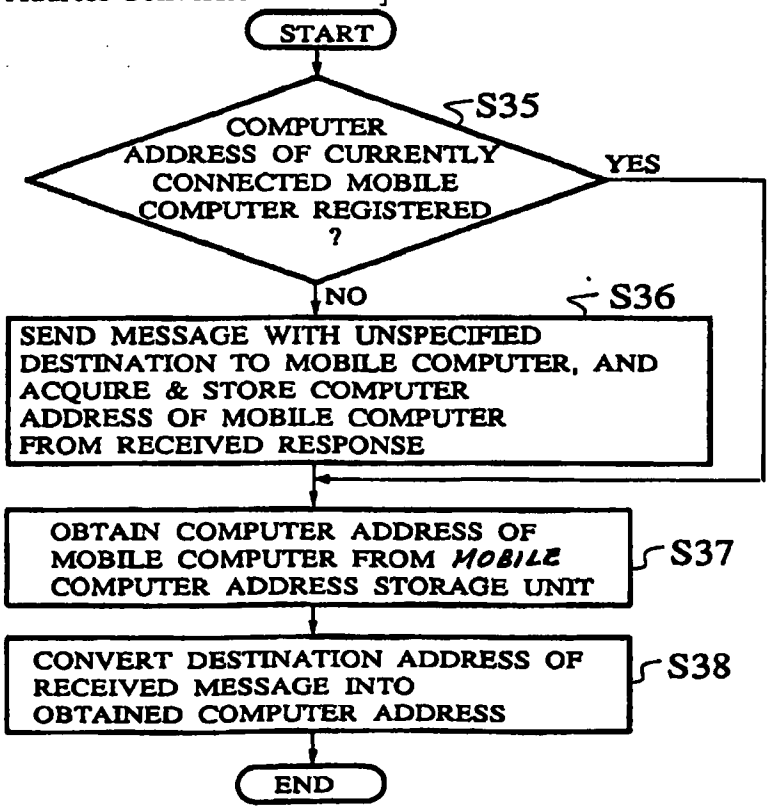

NETWORK
ADDRESS CONVERSION DEVICE
(ADDRESS A1)
Mobile COMPUTER ADDRESS STORAGE UNIT
5
a1
Mobile COMPUTER ADDRESS ACQUISITION UNIT
41
3 1
ADDRESS CONVERSION UNIT
71
a1
8
2 1
MOBILE COMPUTER
M (A2,a1)
(ADDRESS a1)
M (A2,A1)
A1
FIXED ADDRESS STORAGE UNIT
6
ADDRESS CONVERSION DEVICE
(ADDRESS A1)
Mobile COMPUTER ADDRESS STORAGE UNIT
5
a2
Mobile COMPUTER ADDRESS ACQUISITION UNIT
41
3-2
a2
M (A2,a2)
a2
ADDRESS CONVERSION UNIT
71
2 2
MOBILE COMPUTER
M (a11,A2)
M (a2,A1)
(ADDRESS a2)
FIXED ADDRESS STORAGE UNIT
6
1

# FIG. 9

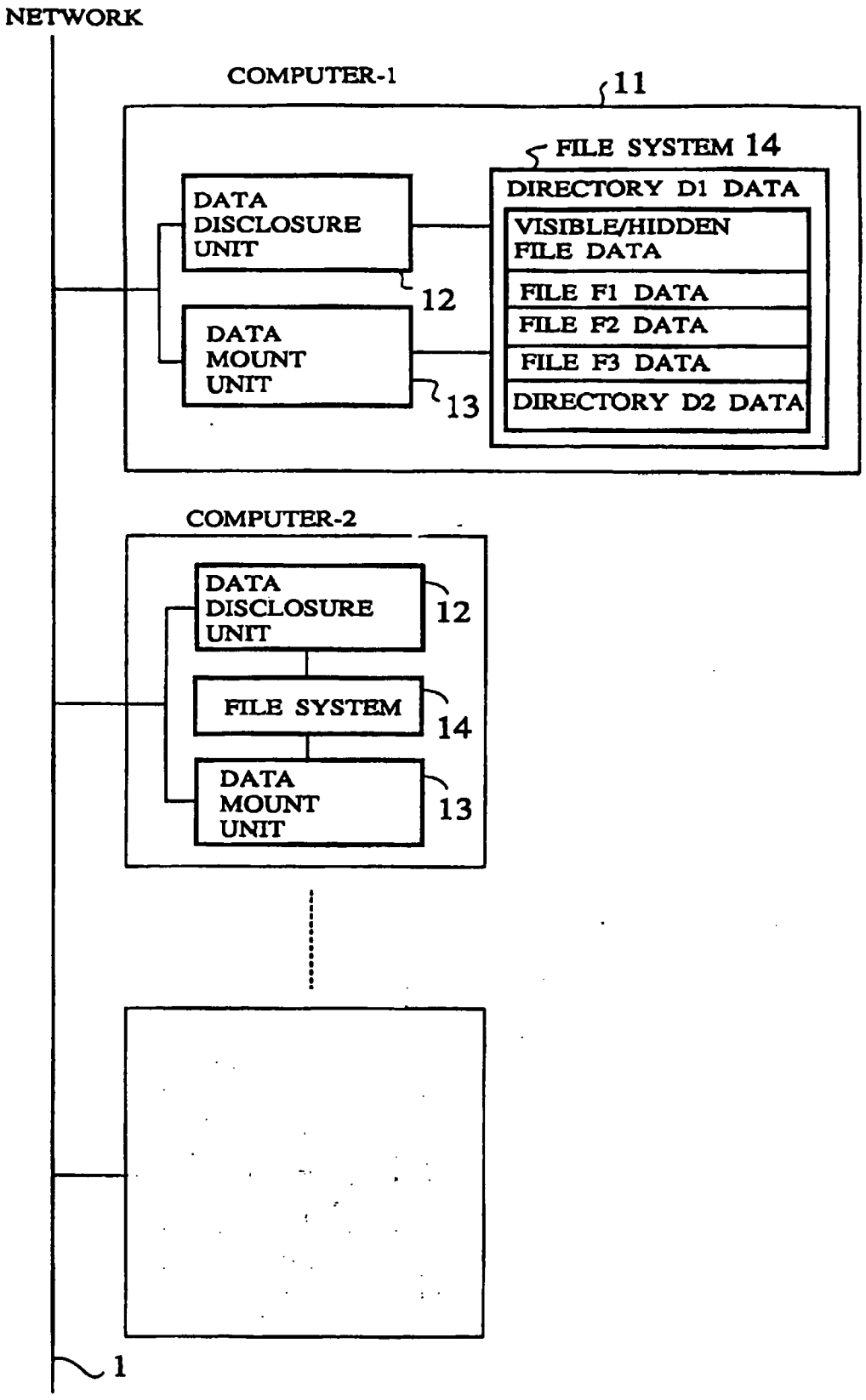
[Message from Mobile Computer]



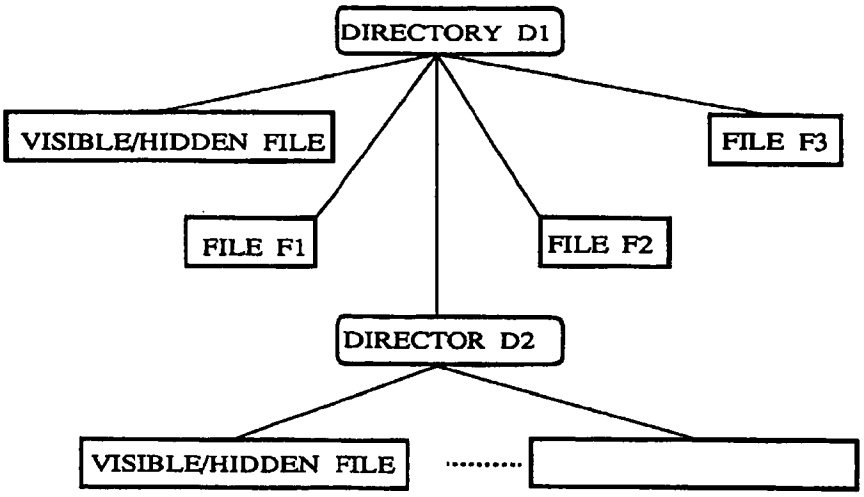

[Message from Other Address Conversion Devices]



# FIG. 10


NETWORK
COMPUTER-1
11
FILE SYSTEM 14
DIRECTORY D1 DATA
VISIBLE/HIDDEN FILE DATA
FILE F1 DATA
FILE F2 DATA
FILE F3 DATA
DIRECTORY D2 DATA
DATA DISCLOSURE UNIT
12
DATA MOUNT UNIT
13
COMPUTER-2
DATA DISCLOSURE UNIT
12
FILE SYSTEM
14
DATA MOUNT UNIT
13
1

# FIG. 11



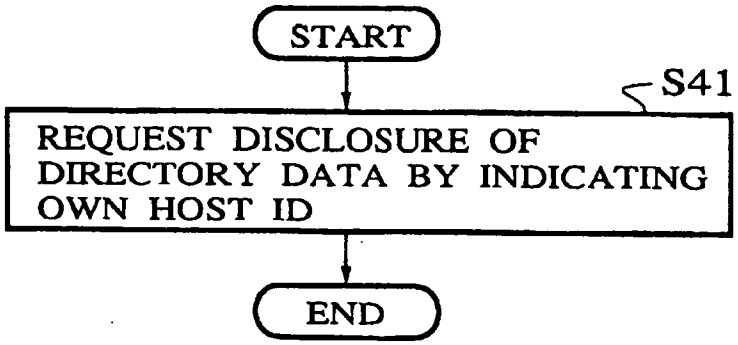

# FIG. 12

VISIBLE/HIDDEN FILE

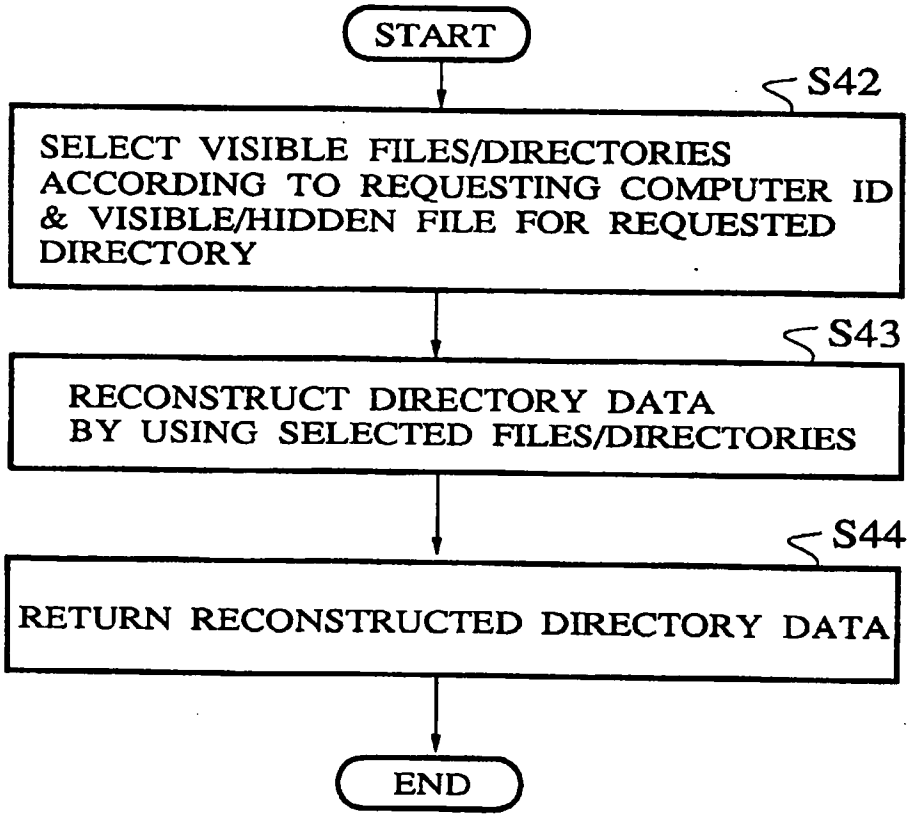
| | |
|---|---|
| FILE F1 | host1, host2, usr1, usr3 |
| FILE F2 | host2, usr2 |
| FILE F3 | host3, usr1 |
| DIRECTOR D2 | host1, usr3 |

# FIG. 13

[Data Mount Unit]




[Data Disclosure Unit]



## CERTIFICATE OF TRANSLATION

I, Mayu Suzuki, a qualified translator fluent in Japanese and English working on be half of Oblon, Spivak, McClelland, Maier & Neustadt, LLP, hereby declare that to the best of my knowledge, the attached documents in English are true and accurate translations of I) Japanese Patent Publication No. JP08070300; and 2) the Japanese Patent Publication No. JP09305155.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Mayu Suzuki
Translator
Oblon, Spivak, McClelland, Maier & Neustadt, LLP
1940 Duke Street
Alexandria, VA 22314
(703) 412-5929 (Direct Dial)

11.25.2009
Date